Optimization Techniques for Detecting Blackhole attack and Securing Mobile Ad-hoc Network(MANET)

A Synopsis submitted to the

School of Computer Science and Application

IIMT University, Meerut

Impartial fulfillment for the award of the Degree of
Doctor of Philosophy

Submitted by

MANOJ GUPTA

Roll No. – 2299002005

Enrolment No. - IIMTU/2299005

Under the Guidance of

Dr. Tarun Kumar Vashishth
Associate Professor (SoCSA)
(IIMT University, Meerut)

School of Computer Science & Applications IIMT University, Meerut(U.P.)

Optimization Techniques for Detecting Blackhole attack and Securing Mobile Ad-hoc Network(MANET)

Introduction:

A promising communication paradigm for a variety of applications, such as military operations, disaster relief, and mobile sensor networks, has evolved called Mobile Ad-hoc Networks (MANETs). MANETs, in contrast to conventional wired networks, are autonomous, Mobile nodes used in decentralised networks constantly assemble a network without utilising any established structure. Because of this distinctive quality, MANETs are extremely versatile and scenario-adaptive. However, MANETs are vulnerable to several security risks, including blackhole attacks, because they lack a centralised authority and communicate cooperatively.

MANETs are self-configuring networks that rely on the cooperation of participating nodes for efficient communication. MANETs are also vulnerable to other security threats, such blackhole attacks, where malicious nodes cause havoc on the network by erratically deleting or changing messages. For MANETs to have dependable and secure connectivity, blackhole attack detection and defence are crucial. The purpose of this study is to defend against blackhole assaults.

The research begins by conducting a comprehensive review of existing literature on blackhole attack detection and mitigation techniques in MANETs. It identifies a research gap regarding the specific utilization of the AODV algorithm for this purpose. The study proposes an approach that incorporates AODV as the routing protocol while enhancing it with mechanisms to detect and defend against blackhole attacks. To evaluate the effectiveness of the proposed approach, a simulation-based methodology is employed. The study takes into account a variety of network scenarios, such as varied network sizes, node densities, and traffic patterns. To evaluate the effect of blackhole attacks on network performance are assessed. Additionally, the detection accuracy and overhead of the AODV algorithm in identifying and mitigating blackhole attacks are evaluated.

The findings highlight the strengths and limitations of the AODV algorithm for detecting and securing against blackhole attacks in MANETs. The research demonstrates that AODV can effectively detect and mitigate blackhole attacks, significantly improving network performance under attack conditions. However, the study also identifies certain scenarios where the algorithm may exhibit limitations or inefficiencies. Based on the research outcomes, recommendations are provided for optimizing the performance of the AODV algorithm in blackhole attack detection and mitigation. The research suggests potential enhancements such as the integration of reputation-based systems, trust models, or intrusion detection techniques into AODV to enhance its effectiveness against blackhole attacks.

The research contributes to the field by providing insights into the application of the AODV algorithm for blackhole attack detection and mitigation in MANETs. The findings inform the development of more robust and resilient routing protocols specifically tailored to the challenges

of MANET environments, thereby enhancing the security and reliability of communication in these networks.

A hostile node known as a blackhole falsely presents denial-of-service (DoS) assault known as a "blackhole attack." A blackhole selectively removes or alters packets as traffic is drawn towards it, effectively disrupting regular routing and jeopardising the network's availability and integrity. To guarantee dependable and secure communication in MANETs, blackhole attacks must be identified and protected against.

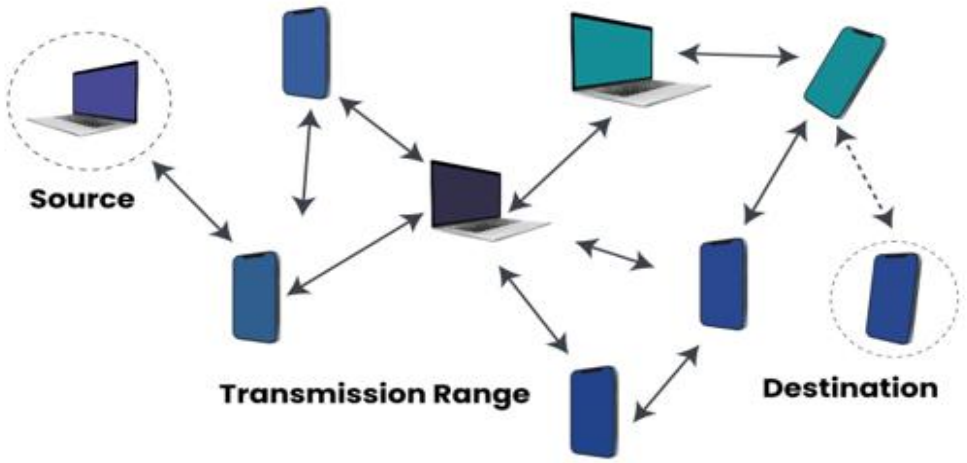

Fig. 1 *Manet Network*

Over the years, numerous research efforts have been dedicated to mitigating the effects of blackhole attacks in MANETs. Various detection and mitigation techniques have been proposed, including intrusion detection systems, secure routing protocols, and trust-based mechanisms. However, the effectiveness of these techniques varies, and there is still a need for further exploration and evaluation of different approaches to tackle the specific challenges posed by blackhole attacks in MANETs.

One of the most popular routing algorithms in MANETs is the Ad-hoc On-Demand Distance Vector (AODV) method. The on-demand routing algorithm AODV creates routes only when they are required, minimising routing overhead and sparing network resources. In order to provide dynamic routing in MANETs, it makes use of route discovery and management techniques. Although AODV has received a lot of attention for general routing needs in MANETs, its applicability and effectiveness for spotting and defending against blackhole attacks have not received as much attention.

By examining the efficiency of the AODV algorithm for identifying and defending against blackhole assaults in MANETs, this research intends to close this gap. The project aims to improve the algorithm with additional methods to recognise and counteract blackhole assaults by exploiting the intrinsic properties of AODV, such as its route finding and maintenance processes.

The objectives of this research are as follows:

1. **Evaluate the quality of the AODV algorithm when there are assaults from black holes:** When blackhole attacks are launched in the network. This evaluation will provide insights into the algorithm's effectiveness in maintaining network connectivity and preserving communication quality under attack conditions.

2. **Develop mechanisms to detect blackhole attacks in AODV:** The research will propose and investigate mechanisms to detect the presence of blackhole nodes within the AODV algorithm. These mechanisms may include monitoring and analyzing packet behaviour, evaluating routing metrics, or utilizing neighbouring node information. The effectiveness of these detection mechanisms will be evaluated and compared to existing approaches.

3. **Enhance AODV to secure against blackhole attacks:** Building upon the detection mechanisms, the research will propose enhancements to the AODV algorithm to mitigate the effects of blackhole attacks. These enhancements may involve dynamically adapting routing decisions based on detected blackhole nodes, establishing alternative routes, or implementing secure communication mechanisms to prevent packet modification.

To achieve these objectives, the research will adopt a simulation-based methodology. Various network scenarios will be considered, encompassing different network sizes, node densities, and traffic patterns. The effectiveness of the AODV algorithm's detection and mitigation of blackhole attacks, as well as its effect on network performance under typical operating settings, will be assessed both with and without the proposed enhancements.

The outcomes capabilities and limitations of AODV algorithm for detecting and securing against blackhole attacks in MANETs. The findings will provide insights into the effectiveness of the proposed detection and mitigation mechanisms and their impact on network performance. Furthermore, the research will inform the development of more robust and secure routing protocols tailored specifically to the challenges of MANET environments, thus enhancing the security and reliability of communication in these networks.

To sum up, blackhole attacks are a serious risk to the dependability and security of communication in MANETs. AODV algorithm detects and defends against blackhole assaults. Through assessing AODV's performance in the face of blackhole attacks, creating detection strategies, and suggesting improvements to lessen the impact of these attacks, this research seeks to improve MANET communication security and dependability, allowing for successful deployment in a range of real-world situations.

Research Gap:

While research has been done on identifying and guarding against blackhole incidents, there is still a significant research vacuum concerning the effectiveness of the AODV (Ad-hoc On-Demand Distance Vector) algorithm especially for mitigating blackhole attacks in MANETs.

1. **Limited focus on AODV algorithm:** Despite the fact that a number of routing protocols for MANETs have been put out, AODV is a well-liked and effective routing algorithm. There is, however, a dearth of thorough research examining the use of the AODV algorithm for detecting and defending against blackhole assaults in MANETs.

2. **Insufficient evaluation of AODV's effectiveness against blackhole attacks:** While some research has investigated the performance of AODV in terms of general network metrics, such as packet delivery ratio, end-to-end delay, and throughput, there is a limited understanding of how well AODV specifically for identifying and defending against blackhole attackers in MANETs.

3. **Lack of consideration for real-world scenarios and practical constraints:** Many existing studies on blackhole attack detection and security in MANETs focus solely on theoretical analysis or simulations. However, real-world scenarios present various challenges and constraints, such as limited network resources, node mobility, and dynamic network topology. There is a need for research that investigates the performance of the AODV algorithm under realistic conditions and incorporates practical considerations.

4. **Exploration of hybrid approaches:** While AODV is known for its efficient on-demand routing, it may benefit from the integration of complementary techniques or hybrid approaches for blackhole attack detection and mitigation. Research is required to explore the potential of combining AODV with other mechanisms, such as reputation-based systems, trust models, or intrusion detection techniques, to enhance its effectiveness against blackhole attacks in MANETs.

By filling up these research gaps, we may acquire a better understanding of the AODV algorithm's strengths and weaknesses in terms of identifying and thwarting blackhole assaults in MANETs. Additionally, it will offer insightful information for creating routing protocols that are more durable and sturdier, particularly designed to meet the demands of MANET settings.

Literature Review:

Because MANETs are dispersed, they are susceptible to several security risks, such as blackhole attacks. When a malicious node pretends to have the quickest path to a target, it attracts all network traffic and then drops or manipulates the data, resulting in a blackhole attack. To address this issue, researchers have proposed various solutions, including the utilization of the Ad-hoc On-demand Distance Vector (AODV) routing algorithm. This literature review aims to explore and summarize the existing research on detecting blackhole attacks and securing MANETs using the AODV algorithm.

The MANET, which is particularly vulnerable in comparison to infrastructure-based networks due to its mobility and shared broadcast nature, is presented by Kumar and Kumar (2015) with a more effective method for detecting a black hole attack with lower communication costs. As a black hole attack can be successfully deployed by an adversary in the network. It is clear that the suggested work is safer than the current options. We also contrasted its efficiency with that of the common AODV routing protocol. The experimental results demonstrate that the suggested approach is superior than traditional AODV. [1]

The fundamental basis of Jain and Tokekar's (2015) proposed method lies in the AODV protocol's caching mechanism for the First Route Reply (RREP). Through simulation, the efficiency of the routing protocol has been enhanced. [2]

A defence strategy against a coordinated attack by numerous black hole nodes in a MANET was presented by Sen et al. (2011). Results from the simulation run on the suggested method show how effective the mechanism is at detecting the assault while preserving a respectable level of network throughput. [3]

The dynamic training method, which Kurusawa et al. (2007) suggest, uses training data that is updated on a frequent basis to discover anomalies. The simulation results demonstrate how effective our plan is when compared to traditional plan. [4]

Yerneni and Sarje (2012) propose a protocol that detects attacks based on the volume of Route requests and Route replies transmitted by nodes. Our research indicates that enhanced protocols can enhance packet delivery rates even in the presence of attacks. [5]

In depth discussion of routing security difficulties and the issue of coordinated attacks by numerous black holes acting in concert in MANET is provided by Min et al. (2009). The message authentication code (MAC) and the pseudo random function (PRF), two authentication mechanisms based on the hash function, are proposed to provide quick message verification and group identification, identify multiple cooperating black holes, and find safe routing avoiding cooperative black hole attack. [6]

The fundamental concept relating to the application of the AODV protocol and the effects of the grey hole attack on adhoc networks are described by Chandure and Gaikwad (2012). Adhoc networks are networks of mobile and wireless nodes that exchange information without the use of an infrastructure. A wireless multihop network, referred to as a mobile ad hoc network, has the capability to operate independently. A node exhibiting the behaviour of selectively dropping and

forwarding data packets is identified as a grey hole.It does this after responding to a route request message by claiming to have the quickest way to the target node. Our system assists in network security by identifying and responding to any node's harmful activity. We can effectively reduce attacks on integrated MANET-Internet communication thanks to the results. A simulation will take place. [7]

Renold and Parthasarathy (2012) proposed a technique capable of detecting a black hole attack. The effectiveness of the reliable AODV routing protocol is evaluated through performance metrics such as packet delivery ratio, throughput, and average end-to-end delay. The assessment was conducted using the QualNet 5.0 simulator, evaluating the dependable AODV under the influence of a black hole attack. [8]

In conclusion, blackhole attacks pose a significant threat to the security and performance of MANETs. Existing solutions employ various detection and mitigation techniques, but they have certain limitations. The proposed research aims to address these limitations by enhancing the AODV algorithm to effectively detect and secure against blackhole attacks in MANETs. By developing a robust mechanism, the research aims to improve the overall security and reliability of communication in MANETs, enabling their successful deployment in various real-world scenarios.

Proposed Model:

1. **Network Setup:** The study framework is based on the assumption of MANET environment with mobile nodes interacting with one another decentralized. The AODV algorithm is used by the selected routing technique because it is effective in creating and maintaining on-demand routes.

2. **Blackhole Attack Detection Mechanism:** To detect blackhole attacks, the proposed model incorporates a novel detection mechanism within the AODV algorithm. *The mechanism operates as follows:*

   a. **Packet Behavior Analysis:** The detection mechanism monitors the behavior of packets exchanged within the network. It analyzes packet reception and forwarding patterns to identify any nodes that exhibit suspicious or abnormal behavior.

   b. **Routing Metric Evaluation:** The mechanism evaluates routing metrics, such as hop count, delay, and route stability, to detect discrepancies caused by blackhole nodes. Nodes that deviate significantly from the expected routing metrics are flagged as potential blackhole attackers.

   c. **Neighbour Node Information:** The detection mechanism utilizes information from neighboring nodes to assess the trustworthiness of individual nodes in the network. By considering the reputation or trust levels of neighboring nodes, the mechanism can identify potential blackhole nodes based on their reputation or trustworthiness scores.

3. **Blackhole Attack Mitigation and Security Enhancement:** The suggested model uses techniques to lessen the effects of the assault and boost network security if a blackhole node is discovered. *These mechanisms include:*

   a. **Dynamic Routing Adaptation:** Upon detecting a blackhole node, the AODV algorithm dynamically adapts its routing decisions to avoid routing packets through the compromised node. Alternative routes are established or existing routes are modified to bypass the blackhole node, ensuring packet delivery to legitimate destination nodes.

   b. **Alternative Route Establishment:** The model includes a mechanism for establishing alternative routes in case the primary route is compromised by a blackhole attack. This mechanism utilizes the information gathered from neighbouring nodes to select reliable and secure alternative routes, ensuring uninterrupted communication in the presence of blackhole attacks.

   c. **Secure Communication:** To prevent packet modification by blackhole nodes, the model enhances the AODV algorithm with secure communication mechanisms. These methods might encompass the utilization of cryptographic methods, such as digital signatures or message authentication codes, to guarantee the integrity and authenticity of the transmitted packets.

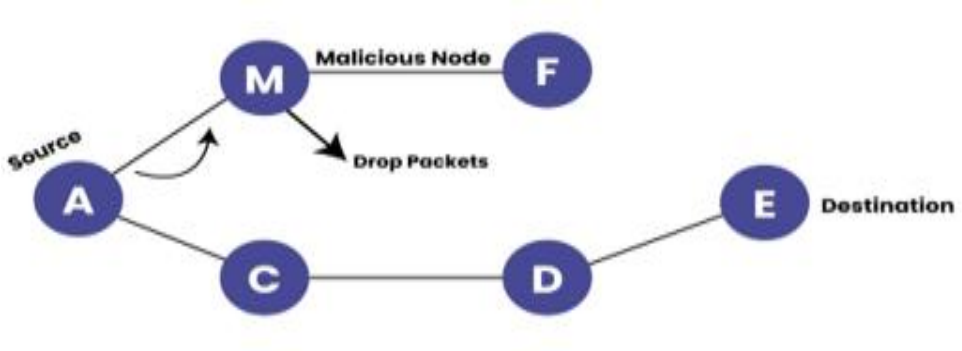

Fig.2*. Blackhole Attack*

4. **Evaluation and Performance Analysis:** The proposed model undergoes extensive evaluation and performance analysis to assess its effectiveness in detecting blackhole attacks and securing the MANET. *The evaluation process involves:*

   a. **Simulation-based Methodology:** The model is implemented in a simulation environment that mimics real-world MANET scenarios. Various network parameters, such as network size, node density, and traffic patterns, are considered to evaluate the model's performance under different conditions.

   b. **Evaluation Criteria:** Metrics including the flow of packets ratio, entirety latency, throughput, and network overhead are used to assess how effective the model is. These

metrics shed light on how well the suggested strategy works to reduce the effects of blackhole assaults and preserve dependable communication inside the MANET.

c. **Comparative Analysis:** The effectiveness of the suggested model is contrasted with that of current approaches. This evaluation shows the model's superiority, if any, in terms of detection accuracy, network performance, and security and identifies the model's advantages and disadvantages.

By implementing and evaluating the proposed model, the research aims to contribute to the field by providing a comprehensive solution for detecting and securing against blackhole attacks in MANETs using the algorithm. The model's effectiveness in mitigating blackhole attacks and improving the security and reliability of communication in MANETs will enhance the understanding and of secure routing protocols for MANET environments.

References:

[1] Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science*, *48*, 472-479.

[2] Jain, A. K., & Tokekar, V. (2015, January). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In *2015 International Conference on Pervasive Computing (ICPC)* (pp. 1-6). IEEE.

[3] Sen, J., Koilakonda, S., & Ukil, A. (2011, January). A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. In *2011 Second International Conference on Intelligent Systems, Modelling and Simulation* (pp. 338-343). IEEE.

[4] A. Jamalipour, N. Kato, S. Kurosawa, H. Nakayama, H. Kato, N. Jamalipour, Y. Nemoto (2007). AODV-based mobile ad hoc networks blackhole attack detection using dynamic learning. Journal of Network Security, 5(3), 338-346.

[5] Yerneni, N. R., & Sarje, A. K. (2012, July). Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc. In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)* (pp. 1-5). IEEE.

[6] Min, Z., and Jiliu, Z. (May 2009). For mobile ad hoc networks, cooperative black hole attack defence. On pages 26–30 of the 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE.

[7] O. V. Chandure and V. T. Gaikwad (2012). AODV routing protocol for the detection and prevention of grey hole attacks in mobile ad-hoc networks. 41(5), 27–32, International Journal of Computer Applications.

[8] Renold, A. P., & Parthasarathy, R. (2012, August). Source based trusted AODV routing protocol for mobile ad hoc networks. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (pp. 1271-1275).